

UNITED STATES DISTRICT COURT

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
One Seagate 2TB external hard drive

)
)
)
)
)
)

Case No. 19-mj-1016

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York (identify the person or describe property to be searched and give its location): One Seagate 2TB external hard drive, which is more fully described and pictured in Attachment A which is attached hereto and incorporated by reference herein.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): Evidence pertaining to violations of Title 22, United States Code, Section 2778, and Title 18, United States Code, Sections 371, 1343, and 554, as more fully set forth in Attachment B which is attached hereto and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 371, 1343, 554 and 22 U.S.C. 2778, and the application is based on these facts: SEE AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Jarrod A. Randle, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/15/19

City and state: Buffalo, New York


Judge's signature
JEREMIAH J. MCCARTHY, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jarrod A. Randle, being duly sworn, depose and state:

I. INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), and have been so employed for approximately 16 years. Prior to my employment with HSI, I was employed as a Special Agent with U.S. Secret Service for approximately one year. I am a graduate of the Federal Law Enforcement Training Center in Glynco, Georgia, where I was trained in, among other things, criminal investigative techniques and export-control investigations. I have also received formal training in the laws and regulations relating to the Arms Export Control Act (“AECA”), 22 U.S.C. § 2778, and the International Traffic in Arms Regulations (“ITAR”), 22 CFR 120-130. I am currently assigned to the Special Agent in Charge, Buffalo, New York office to investigate violations of federal criminal law, including Title 18 and Title 22.

2. I make this affidavit in support of an application for a warrant to search a Seagate 2TB external hard drive (hereinafter ‘SUBJECT PROPERTY”), which is more fully described and pictured in **Attachment A**. Specifically, the SUBJECT PROPERTY was provided to HSI by Canadian authorities pursuant to a Mutual Legal Assistance Treaty (MLAT) request. The SUBJECT PROPERTY contains electronic data obtained by Canadian authorities during the execution of a Canadian search warrant on various electronic

storage devices found in the possession of Aydan Sin (“SIN”). The actual electronic devices were returned to SIN by the Canadian authorities.

3. The statements contained in this affidavit are based on my involvement in this investigation, as well as information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is being submitted for the limited purpose of seeking a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 22, United States Code, Section 2778, and Title 18, United States Code, Sections 371, 1956, and 554, exists on the SUBJECT PROPERTY.

II. STATUTORY BACKGROUND

4. The United States Arms Export Control Act, Title 22, United States Code, Section 2778 (“AECA” or the “Act”) authorizes the President to control the export of defense articles and services from the United States. The Act requires every person engaged in the business of exporting defense articles from the United States to obtain a license or other approval from the United States Department of State (“Department of State”). 22 U.S.C. § 2778(b)(1)(A)(I). The regulations promulgated pursuant to the Act, known as the International Traffic in Arms Regulations, Title 22, Code of Federal Regulations, Parts 120-13 (“ITAR”), define exporting to include, among other things: “[s]ending or taking a defense article out of the United States in any manner” 22 C.F.R. § 120.17.

5. Defense articles that are subject to such licensing requirements are designated on the United States Munitions List ("USML"). Those designations are made by the Department of State with the concurrence of the United States Department of Defense ("Department of Defense"). (22 U.S.C. § 2778(a)(1); 22 C.F.R. § 120.2.).

6. Category I of the USML includes firearms, close assault weapons and combat shotguns, as well as certain components, parts, accessories, attachments, and associated equipment related to the same. (22 C.F.R. § 121.1.).

7. Unless specifically exempted, the AECA and its attendant regulations, the ITAR, require persons engaged in the export of defense articles covered by the USML to register with the Directorate of Defense Trade Controls ("DDTC") of the Department of State and obtain an export license from the DDTC before exporting defense articles from the United States by any means. (22 U.S.C. § 2778(b)(2); 22 C.F.R. §§ 120.1, 120.17.) (22 U.S.C. § 2778(b)(2); 22 C.F.R. §§ 120.1, 120.17.) Moreover, the DDTC maintains records of companies and individuals who have registered with the DDTC and applied for and received export licenses.

III. THE INVESTIGATION AND FACTUAL BASIS

8. As set forth in more detail below, the current investigation involves the attempted illegal export of controlled munitions from the United States to the United Arab Emirates and Colombia by three citizens and residents of Canada, Charan Singh ("SINGH"), SIN, and Guy Deland ("DELAND"). Specifically, these three defendants have taken

significant steps to cause the exportation of 9mm Glock pistols and Uzi submachine guns (“Uzis”) by communicating and meeting with an HSI undercover agent, acknowledging the illegality of the attempted exports, providing an encrypted BlackBerry device for the purposes of secure communications, and wiring approximately \$70,000 USD from Canada to the United States as a 50% down payment for the unlicensed export.

A. Initial Contacts Between Singh and the HSI Undercover Agent

9. In November 2016, an individual using the name “Charlie” initiated communications with an HSI undercover agent (the “UCA”). “Charlie” was subsequently identified as SINGH, who was born in Malaysia but currently resides in Canada and has Canadian citizenship. SINGH contacted the UCA from telephone number 514-586-3802, with a Montreal, Quebec, Canada-based area code. During the telephone conversation, SINGH and the UCA discussed a potential purchase of U.S.-origin firearms and agreed to communicate via cell phone text message and e-mail message. SINGH also told the UCA that he lived in Montreal, and asked to meet with the UCA in the future to discuss the potential deal.

10. On November 22, 2016, after SINGH had made initial telephone contact with the UCA, the UCA also received text messages from SINGH from a second telephone number, 647-649-0853. On the same date, the UCA received e-mails from SINGH indicating that he was looking to purchase Glock and Beretta handguns to be shipped to Dubai UAE, and they wanted five (5) of each pistol. Follow-up conversations with Singh revealed that he wanted to acquire Glock and Beretta handguns to export from the United States to Dubai,

United Arab Emirates (“UAE”). In a November 23, 2016 e-mail, the UCA outlined the proper method to export firearms from the U.S. in compliance with International Traffic in Arms Regulations (“ITAR”). This explanation included details regarding the required licensing process through the U.S. Department of State. In response to that e-mail, SINGH inquired whether there “was any other way to do it” because this transactions would only be a trial and they would have much bigger orders after this transaction was complete.

11. During a November 30, 2016 call, SINGH again asked if it was necessary to get a license to export the munitions. The UCA explained that other methods existed but would not be legal. The UCA then asked if SINGH was asking him to circumvent the U.S. export licensing requirements or if he wanted to proceed with obtaining an export license. SINGH responded that he did not care about the paperwork. SINGH said his people did not care which way or how the UCA got the guns to Dubai as long as they got there. During that same call, SINGH said that he would be obtaining a list of guns that his customers wanted. According to SINGH, much larger orders for these types of guns (including pistols, machine guns, and grenades) would be forthcoming once the Dubai order was fulfilled. When the UCA asked about specific models that they wanted shipped to Dubai, SINGH responded that they mostly wanted “pistols and automatics”. During the call, SINGH also explained that his group was trying to beat out another party that has been supplying these “customers”, and once the UCA completed this small trial run, orders to follow will be much larger and worth a half million or a million dollars apiece.

B. The UCA Begins Communicating with SIN

12. On December 2, 2016, the UCA received a telephone call from SINGH, during which he advised the UCA that he wanted to introduce the UCA to his partner.

13. On December 5, 2016, the UCA received another telephone call from SINGH. During the conversation SINGH asked if the UCA could come to Montreal to meet with his partner to discuss the gun deal. SINGH said his partner was from "BC" or British Columbia and will be in Montreal for the next ten (1) days.

14. In a follow-up call on December 7, 2016, SINGH introduced the UCA to his partner, "ANDY." "ANDY" then got on the telephone line and began a conversation with UCA. Royal Canadian Mounted Police ("RCMP") surveillance led to identification of "ANDY" as SIN, also known as Hon Chak Gordon Sin.

15. During that conversation, SIN told the UCA that he wanted to purchase 9mm pistols from the UCA and have them exported to Dubai. SIN told the UCA that after the order of guns to Dubai was completed, many other gun orders would follow including orders to Colombia, Canada, Japan, and Australia. SIN also told the UCA that he wanted to add "extra other things" and that he would e-mail the UCA what those were. Later on December 7, 2016, the UCA received an e-mail from SINGH indicating that those "extra guns" were mini Uzi submachine guns with "silencers." During the conversation, shipping details were discussed about getting the guns from the U.S. to Dubai. SIN asked the UCA to take care of all the shipping including exporting and receiving the shipment in Dubai and that they simply

wanted to pick the guns up from the UCA once he got them to Dubai. SIN also referred to the guns throughout the conversation as “cars” or “car models.” When payment was discussed, SIN told the UCA that he can pay anywhere in the world, including the UCA’s office in the U.S. When the UCA asked about wire transfers, SIN laughed and stated that his definition of a wire was “cash to cash.” The conversation concluded with SIN asking for an invoice for the purchase and export of those guns to Dubai and asking the the UCA to meet with him in Montreal in the coming days to further discuss the deal.

16. At the request of HSI, RCMP Montreal opened a casefile, began an investigation of SINGH for the purpose of assisting HSI’s investigation, and RCMP agreed to support an undercover meet between the UCA, SIN, and SINGH in Montreal, including conducting surveillance before, during, and after that meeting.

17. Between December 7 and 8, 2016, e-mail communications between the UCA and SINGH continued pertaining to the purchase and export of ten (10) Glock pistols and some Uzis to Dubai. On December 8, 2016, SINGH and the UCA exchanged e-mail messages discussing details of the gun deal. On that same date, RCMP conducted surveillance and observed SINGH, SIN, and a third man, later identified as DELAND meeting together at a Tim Horton’s coffee shop in SINGH’s hometown of L’Ile-Perrot, Quebec.

18. On December 9, 2016, the UCA e-mailed an invoice entitled “Purchase Order” to SINGH. The invoice included the cost of 40 Glock 26 pistols, 15 IMI mini Uzis, 15 Uzi

suppressors with adapters, and sales tax for a total of \$96,243.75 USD. Also attached to the invoice was an ITAR End-Use Statement and a U.S. Department of State DSP-83 form to apply for an export license. Later that day, the UCA received a telephone call from SINGH, who said SIN was trying to get ahold of the UCA regarding the invoice.

19. The UCA also received a December 9, 2016 telephone call from SIN. During the call, SIN said that he received the UCA's e-mail with the invoice and wanted to know what the additional charge would be for conducting the transaction another way. When the UCA said there was a right way and wrong way to ship the guns, SIN stated that he wanted to do it "the wrong way," without the export paperwork. SIN then asked the UCA to e-mail a new invoice including the UCA's "service fee" for shipping the guns the "wrong way." After the conversation, the UCA sent an e-mail to SINGH's account with an attachment of a revised Purchase Order, including an additional "service fee" of \$26,550 for conducting the transaction in violation of U.S. export laws. The new total amount of the revised invoice was \$122,793.75 USD.

C. Meeting in Montreal with Guy Deland

20. As mentioned above, during a December 5, 2016 telephone conversation with SINGH, SINGH requested that the UCA travel to Montreal, Quebec, Canada, to meet with him and his partner "ANDY" (SIN). SINGH advised the UCA that SIN would be in town from British Columbia, Canada, for the next ten (10) days and wanted to meet with the UCA to discuss the gun transaction.

21. On December 11, 2016, the UCA received an e-mail from SIN, and they continued to communicate via e-mail and text message (with SIN communicating from that same e-mail address and a new telephone number 438-920-8599) in anticipation of the meeting in Montreal. In these communications SIN described himself as Chinese.

22. On December 14, 2016, after continued communication with SIN, the UCA met in Montreal with a partner of SIN's who called himself "Mark" (later identified as Guy DELAND). Upon meeting DELAND, he and UCA began talking about making plans to meet ANDY. At one point UCA indicated that he expected to meet with a Chinese guy, to which DELAND told the UCA that SIN had intentionally misled the UCA as to who the UCA would be meeting with. During the meeting, DELAND and the UCA discussed details about purchase, export, and delivery of the Glock pistols and Uzis. Also during this meeting, DELAND stated that larger gun orders to various countries would follow if the UCA successfully delivered the first order to Dubai. DELAND referenced the Purchase Order that the UCA had e-mailed to SINGH and asked the UCA numerous questions about the proposed transaction, including questions about how the UCA would obtain the guns, when delivery would occur, what shipping methods would be used, and what would happen if the shipment was delayed or seized. RCMP provided surveillance assistance before, during, and after the meeting. As part of this surveillance, RCMP observed an individual matching the description of SIN parked in a rental vehicle outside of the meeting location, a hotel lobby bar in downtown Montreal. RCMP review of rental records for the car, showed it had been rented in SIN's name, with one of SIN's telephone numbers given as the contact number. After the

meeting, RCMP observed DELAND exit the meeting location and enter that same vehicle driven by SIN.

23. At this December 14 meeting, the UCA and DELAND also discussed that DELAND and his associates would pay the UCA for the guns in the U.S. When the UCA discussed the export documentation that needed to be completed to facilitate the transaction, DELAND explained that he and his people did not want to sign any paperwork, and that their signature was “a bag of cash.” The UCA explained to DELAND that what they were asking him to do was illegal, and that the UCA had e-mailed the paperwork and government forms to conduct the transaction the legal way. DELAND admitted that the risk the UCA was taking was why he and his co-conspirators were willing to pay the UCA a “service fee.”

24. Also at this meeting, DELAND told the UCA that he and his associates would be giving the UCA an encrypted BlackBerry device, which was not easily traceable by police, to communicate with them about the gun deal. DELAND said he and his partners would give the UCA a down-payment representing 50% of the total price reflected on the Purchase Order that the UCA had e-mailed to them.

25. At the conclusion of the meeting, DELAND stated that the UCA would be communicating with DELAND about the gun order going forward on the same phone number he had used to speak with ANDY.

D. Encrypted Mobile Phone Provided to the UCA

26. On December 15, 2016, the UCA received a telephone call from SINGH from 514-586-3802. The UCA asked SINGH about the encrypted telephone that DELAND previously indicated the UCA would receive. SINGH mentioned that the phone could erase automatically and would provide a safer way to communicate openly. SINGH said the phones usually come from "BC" (referring to British Columbia). SINGH also told the UCA that SIN was DELAND's "boss." SINGH explained that SIN is very busy working on all sorts of deals from the western part of "BC," and that DELAND was a guy that SIN used to make deals in the Montreal area. SINGH told the UCA that SIN would make the decision about when to move forward with the gun order to Dubai.

27. Throughout December 2016 and January 2017, DELAND continued to communicate with the UCA about completing the gun shipment to Dubai. During a telephone conversation on December 23, 2016, DELAND asked the UCA if the serial numbers on the guns would be removed. DELAND specifically asked whether, if the guns had been used in a breaking and entering or to hold someone up, their serial numbers could be traced to the UCA. DELAND stated that he would ask his associates if they wanted the serial numbers removed. In a later conversation, DELAND told the UCA that "they" wanted the serial numbers removed.

28. In December 2016 and January 2017, the UCA, at the request of DELAND and SIN, e-mailed several revised Purchase Orders to DELAND and SIN for the shipment of 40 Glock 26 pistols and 15 mini Uzi submachine guns with suppressors to Dubai. The revised

Purchase Orders reflected changes to the UCA's "service fee," as well as charges associated with splitting the order between Dubai and a second destination (Colombia), at SIN's request. In a text message dated December 29, 2016, DELAND told the UCA that "my guy" (referring to SIN) wanted 10 guns in Dubai and the rest "South of u." Later in January 2017, DELAND, through text messages and telephone calls, asked the UCA to e-mail a revised Purchase Order for three Glocks and two mini Uzis to Dubai and the rest (37 Glock 26s and 13 mini Uzis) to Cartagena, Colombia. During this time, DELAND sent a text message to the UCA from 438-920-8599 indicating that his e-mail address was aaronbeland@hotmail.com. The revised Purchase Orders were later e-mailed by the UCA to DELAND and SIN.

29. On January 9, 2017, DELAND called the UCA and explained to the UCA that the UCA would be receiving a phone with a special program called "Sky," which would provide a safe communication method to protect all of their people on the network. DELAND explained that two separate passwords would be needed to access the device, and that if one device was compromised then all of the phones on their network would be remotely erased.

30. On January 21, 2017, DELAND sent the UCA a text message stating that the phone would be mailed to the UCA's address in Buffalo, New York. DELAND also indicated that arrangements to deliver a down payment to the UCA for the two gun orders would be made via the encrypted phone device once the UCA received it.

31. On January 30, 2017, an HSI agent picked up a FedEx package that had been mailed to an HSI Buffalo undercover location. The package contained a shipping label indicating it was shipped from an address in Indianapolis, Indiana, but included a Montreal contact telephone number for the shipper. The FedEx package contained a black BlackBerry Q5 mobile telephone.

32. On January 30, 2017, the UCA communicated via text message and telephone conversation with DELAND, who guided the UCA through the process of setting up the BlackBerry device. DELAND instructed the UCA regarding setting up two passwords to access the phone, setup features including self-destruct time frames for text messages, and a “distress password” to delete everything in the phone. DELAND described the “distress password” as a double layer of protection that can be used if a law enforcement officer tries to access the phone. A contact named “Bullion” was pre-loaded into the phone’s contacts, and DELAND indicated to the UCA that “Bullion” was SIN. DELAND also helped the UCA to load DELAND’s contact information into the device under the name “Security Prime.” DELAND told the UCA to use the phone solely for communicating with him and SIN via secure text messages.

E. The Down-Payment

33. Between January 30 and February 7, 2017, the UCA communicated with SIN and DELAND, primarily through the secure BlackBerry device. SIN’s first text message to the UCA on the BlackBerry device read: “Hi my friend. Finally, we can talk to each other freely.” The conversations that followed centered on SIN and DELAND providing a down

payment of \$70,000 USD to the UCA for the shipment of guns to Dubai and Colombia. There was also discussion about timeframes to have the guns shipped to Dubai and Colombia, that SIN would have a “pick up guy” in both locations to receive the guns, and that SIN also wanted the UCA to fill an order of guns to Vancouver, British Columbia, Canada (specifically, for .40 caliber, .357 caliber, and .45 caliber Glock handguns). SIN also asked the UCA how secure the shipment would be and whether SIN would get his money back if there was a “bust on the border” during the shipment. SIN and the UCA also discussed the illegal nature of the gun order, and SIN reiterated that he wanted the order done “the wrong way.”

34. On February 6 and 7, 2017, an HSI Buffalo undercover bank account located in the Western District of New York received two bank wire transfers from a TD Bank account in Canada, each in the amount of \$34,990 USD (for a total of \$69,980 USD), representing 50% of the total purchase price of 40 Glock 26 handguns and 15 mini Uzi submachine guns with suppressors to be shipped to Dubai and Colombia in violation of U.S. export laws.

35. After these wire transfers were received, SIN and DELAND continued to communicate with the UCA, primarily through the aforementioned encrypted device, to discuss completing the current order of guns and subsequent orders of guns to be exported elsewhere. SIN and DELAND specifically asked for an invoice from the UCA for an order of 40 Glock 27 handguns, 40 Glock 38 handguns, and 40 Glock 32 handguns to be exported to Vancouver, and mentioned additional future orders to Holland and Australia.

36. HSI used existing sea freight shipments available from open source information to give the targets the impression that a container containing legitimate goods with their guns co-mingled and concealed among the cargo had been sent to both Dubai and Colon, Panama. Specifically, the UCA told SIN and DELAND that a shipping container containing their order for Dubai had departed the seaport in Newark, New Jersey, on March 18, 2017, destined to arrive at the seaport of Jebel Ali, UAE, on April 15, 2017. The UCA also told SIN and DELAND that a shipping container containing their order for Colombia would be departing the seaport in Newark, New Jersey, destined to arrive at the seaport in Colon, Panama, on March 29, 2017.

F. SIN's Electronic Devices

37. On May 4, 2017, a grand jury sitting in Buffalo, New York, returned an Indictment, Crim. No. 17-CR-90A, charging SIN, DELAND, and SINGH with six criminal offenses relating to the attempted export of firearms and ammunition from the United States. SIN's extradition process has completed, and on December 14, 2018, was arraigned on the charges. DELAND and SINGH remain in the extradition process in Canada. The United States is continuing to investigate whether any other individuals conspired with SIN, DELAND, and SINGH to commit offenses against the United States.

38. On June 21, 2017, pursuant to a provisional arrest warrant, RCMP officers arrested SIN upon exiting his vehicle outside of his residence in Richmond, British Columbia. During the arrest, RCMP officers also lawfully seized miscellaneous documents and the following electronic storage devices in SIN's possession:

- a. One Apple MacBook Pro laptop computer
- b. One Toshiba Portege M200 laptop computer
- c. One Mi Smartphone cellular telephone
- d. One Apple iPhone7+ cellular telephone
- e. One Nexus LG Android cellular telephone
- f. One BlackBerry cellular telephone
- g. One Lexar 16 GB thumb drive

39. During the period of the alleged criminal conduct, SIN resided in Vancouver, British Columbia, but his alleged co-conspirators, SINGH and DELAND, lived in Quebec. Evidence collected during the investigation confirmed that the three co-conspirators regularly communicated with one another via mobile phone, including through the use of special, secure communications applications, and email.

40. Throughout the time period of the alleged criminal conduct, SIN communicated with the UCA via either text message and voice communications on three different identified telephone numbers and via a secure application on a Blackberry device. SIN was also associated with two additional telephone numbers that SIN listed on rental vehicle contracts in December 2016, while in communication with the UCA.

41. During this same time period, SIN also communicated with the UCA via e-mail, which could have been sent via any cell phone or laptop computer.

42. According to information provided by the RCMP, the electronic devices seized from SIN were subject to a subsequent Canadian search warrant. During a Canadian search of the electronic devices, RCMP advised that they uncovered internet searches that were conducted on the Toshiba laptop that related to the illegal export scheme. RCMP also uncovered an invoice and an e-mail created by the UCA on the BlackBerry device seized from SIN. The electronic evidence obtained by the Canadian authorities was placed on the SUBJECT PROPERTY and later provided to HSI pursuant to a MLAT request. Although Canadian authorities have already searched through the electronic evidence contained on the SUBJECT PROPERTY, this search warrant to review the evidence contained on the SUBJECT PROPERTY is being sought out of an abundance of caution.

IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

43. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

44. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

45. There is probable cause to believe that things that were once stored on the SUBJECT PROPERTY may still be stored there for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even

years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media - in particular, computers’ internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

46. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be found on the SUBJECT PROPERTY because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from

a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used, for example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated

camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

47. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

48. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. THE PROPERTY TO BE SEARCHED AND ITEMS TO BE SEIZED

49. Based on the foregoing, there is probable cause to believe that on the SUBJECT PROPERTY, which is more fully described and pictured in **Attachment A**, there is located evidence, fruits and/or instrumentalities of the violations specified in this affidavit.

50. Based on the foregoing, there is probable cause to believe that on the above property the items set out in **Attachment B** will be located stored in electronic form.


VI. CONCLUSION

51. Based upon the above information, I believe that probable cause exists to believe there has been violations of Title 22, United States Code, Section 2778, and Title 18, United States Code, Sections 371, 1956, and 554, and that there is probable cause to believe that on the SUBJECT PROPERTY, which is more fully described and pictured in **Attachment A**, there is located those items set out in **Attachment B**.


52. In consideration of the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT PROPERTY, which is more fully described in **Attachment**

A, authorizing the search of the aforementioned property for the items described in **Attachment B**.

53. Finally, since this affidavit relates to an ongoing criminal investigation and contains the names of individuals who are witnesses and/or targets in this matter, the government respectfully moves this Court to issue an Order sealing, for 60 days unless the Court orders otherwise, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant.


Jarrod A. Randle, Special Agent
Homeland Security Investigations

Sworn to before me this 15th day of
March, 2019.


HON. JEREMIAH J. MCCARTHY
United States Magistrate Judge

ATTACHMENT A
Property to be Searched

The item to be searched is further described and pictured below as follows: One Seagate 2TB external hard drive black in color (hereinafter SUBJECT PROPERTY"). The SUBJECT PROPERTY was provided to HSI by Canadian authorities pursuant to a Mutual Legal Assistance Treaty request, and is currently in the possession of HSI in Buffalo, New York. The SUBJECT PROPERTY contains electronic data obtained by Canadian authorities during the execution of a Canadian search warrant on various electronic storage devices found in the possession of Aydan Sin at the time of his arrest on June 21, 2017. Data from the following devices is contained on the SUBJECT PROPERTY: one Apple MacBook Pro laptop computer, one Toshiba Portege M200 laptop computer, one Mi Smartphone cellular telephone, one Apple iPhone7+ cellular telephone, one Nexus LG Android cellular telephone, one BlackBerry cellular telephone, and one Lexar 16 GB thumb drive.



ATTACHMENT B
The Items to be Searched for and Seized

The items to be searched for and seized on the property listed in Attachment A, are as follows:

For the period of time from January 1, 2016, to June 21, 2017, any and all evidence relating to violations of Title 22, United States Code, Section 2778, and Title 18, United States Code, Sections 371, 1343, and 554, that pertains to the following:

1. Records of telephone calls, including incoming, outgoing, and missed calls, phone contact addresses, email addresses and telephone numbers in directories, documents and files which reflect names, email addresses, physical addresses, telephone numbers, photographs, and objects related to sale/purchase and/or import/export of United States Munitions List ("USML") items
2. Text messages and emails related to the sale/purchase and import/export of USML items, including email attachments.
3. Photographs of BlackBerry messaging pertaining to the sale/purchase and import/export of USML items.
4. Records regarding the ownership and/or possession of data that was placed onto the SUBJECT PROPERTY.
5. Records regarding the sale, offer for sale, purchase, offer for purchase, import, or export of any weapons, firearms, firearm accessories, or firearm components.
6. Records regarding export controlled items on the USML.
7. Information relating to the import/export laws of any country regarding weapons, firearms, firearm accessories, or firearm components.
8. Communications regarding any pending investigations regarding the import, export, sale, purchase, transportation, or possession of any weapons, firearms, firearm accessories, or firearm components.
9. Records regarding international and/or domestic travel.

10. Records about financial transactions relating to the sale, offer for sale, purchase, offer for purchase, import, or export of any weapons, firearms, firearm accessories, or firearm components, to include all bank records, checks, credit card bills, account information, wire transfer of funds, and other financial records.

11. Communications or records regarding organized criminal activity relating to the sale, offer for sale, purchase, offer for purchase, import, or export of any weapons, firearms, firearm accessories, or firearm components.

12. Evidence indicating how and when the devices were accessed or used, to determine the geographic and chronological context of access, use, and events relating to the crimes under investigation and to user of the devices.

13. Records of Internet Protocol addresses used.

14. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

15. Evidence of user attribution showing who used or owned the SUBJECT PROPERTY at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.